aircrack ptw

Posté le Mardi 10 avril 2007 à 11 h 28, Read it in english with Google

Un petit nouveau est sortie le 1er avril, permettant de **cracker un clef WEP beaucoup plus rapidement que les anciens aircrack ou encore aircrack-ng**.

aircrack-ptw, serait capable de **trouver une clef avec seulement 10 000 IVS**, autant dire en moins de 5 minutes dans les meilleurs conditions.

Alors je me suis dit… faut que je test !!!
Allez, **installation** :
Tout d'habord il vous faut les **sources de la librairie pcap** :

```
apt-get install libpcap0.8-dev
```

vous télécharger les source de **aircrack-ptw** sur le site officiel :

```
wget http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/download/aircrack-ptw-1.0.0.tar.gz
tar -zxvf aircrack-ptw-1.0.0.tar.gz
```

Ensuite vous faites un petit

```
cd aircrack-ptw-1.0.0
make
```

voila le programme est compilé et fin près à servir.

C'est la que franchement on se demande si ce n'est pas un poisson d'avril.

Vous prenez quelques **dizaines de millier de IVS** avec **airodump-ng**, attention **sans activer l'option *-ivs*** sinon ça ne marchera pas.
Vous lancez donc :

```
./aircrack-ptw out-0x.cap
```

si votre fichiers contient trop peu de IVS, voila ce que ça va donner :

```
xorax@xorax:~/Desktop/aircrack-ptw-1.0.0$ ./aircrack-ptw out-01.cap
This is aircrack-ptw 1.0.0
For more informations see http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/
xorax@xorax:~/Desktop/aircrack-ptw-1.0.0$
```

Franchement c'est fait à ~~l'arrache~~ j'éspère que quelqu'un va bientôt retoucher ça parce qu'on ce croirait à ~~l'age de pierre~~…

Bref en fait il faut selectionner le fichier *.cap* qui possède le plus d'info (le plus gros). **aircrack-ptw** va selectionner le réseau avec le plus de IVS dans ce fichier et trouver la clef. Et n'éssayer pas de mettre plusieurs fichiers à la suite ça ne marche pas…

Au final, avec un paquet qui trainait dans mes archives, j'ai obtenu

```
xorax@xorax:~/Desktop/aircrack-ptw-1.0.0$ ./aircrack-ptw output-06.cap
This is aircrack-ptw 1.0.0
For more informations see http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/
```

```
allocating a new table
bssid = 00:03:C9:52:3F:89 keyindex=0
stats for bssid 00:03:C9:52:3F:89 keyindex=0 packets=77858
hit with strongbyte for keybyte 6
Found key with len 13: 8D 5D E7 57 70 39 F6 26 13 52 CA 37 05
```

Et j'ai même pas eut le temps de faire ~~joujou~~ avec les fenètre de beryl que la clef était déjà affiché
Non vous voyez bien **avec 78 000 paquet j'ai la clée !**.

Alors là c'est **la fin du WEP**…
Bon il y a encore des limitations, cet outils ne marche que pour les **clef WEP de 40 ou 104 bits**, ça représente 90 % des AP en WEP donc c'est déjà bien.

C'était le bon temps quand même avec le vieux aircrack ont avait plein de couleurs et on regardait toutes les minutes s'il avait pas trouvé la clef avec nos pauvre 500 000 ivs alors que là c'est même plus marrant …

Voila également la version pour **Windows** amélioré, grace à Rorry sur tuto-fr.com :
aircrack-ptw_win32

Également dans les catégories hacking, sécurité, wifi. Vous pouvez suivre les nouveaux commentaires. Vous pouvez ajouter un commentaire, ou faire un trackback sur votre site.

Articles en relation :

- wesside-ng
- WEPBuster : crack WEP automatique
- google : scanner d'adware ?
- ubuntu atheros wifi wpa
- notions de sensibilité-puissance en wifi

45 réponses à "aircrack ptw"

aircrack-ptw *contient sur le sujet* :

[…] Zac nous a fais un petit test lui aussi sur dev.tuto-fr.com Xorax en parle lui aussi […]

le Mardi 10 avril 2007 @ 17 h 50

nefaria
a écrit le Samedi 21 avril 2007 @ 11 h 55 :

eux tu utilise linux ou windows je narive pas a télécharger le soft avec ton lien

XoraX
a écrit le Samedi 21 avril 2007 @ 12 h 11 :

ah c'est du linux
mais y me semble qu'il y a moyen de le compiler sous windows, je vais mater ça

XoraX
a écrit le Lundi 23 avril 2007 @ 8 h 29 :

hop! mate en bas de d'article

XoraX
a écrit le Mardi 22 mai 2007 @ 12 h 06 :

stop aircrack-ptw! la dernière version d'aircrack-ng intègre l'algorithme avec l'option -z

dom
a écrit le Mardi 29 mai 2007 @ 18 h 46 :

salut, comment peut on faire sous mac os pour craquer une clef wep ?
tu sais ?
merci.

XoraX
a écrit le Mardi 29 mai 2007 @ 19 h 18 :

déjà sous windows c'est très difficile alors sur mac…
Mais utilise un live CD linux t'as rien besoin d'installer :
http://www.tuto-fr.com/tutoriaux/tutorial-crack-wep-aircrack.php

hs_force
a écrit le Mardi 12 juin 2007 @ 23 h 10 :

Hello tu peux me dire comment cracker une clé wep je suis sur xp?

XoraX
a écrit le Mercredi 13 juin 2007 @0 h 39 :

même réponse.
Dans 98% des cas tu ne pourra pas faire d'injection de paquet sous windows (sauf si tu a acheter une carte spécial pour ça, ne compte pas l'avoir d'origine sur ton pc). Pas d'injection ça veut dire que tu va recevoir dans le meilleur des cas 40 IVS/seconde (si le gars écoute la radio, à la mule qui tourne, et joue à CS en même temps) or il te faut au moins 35 000 IVS pour pouvoir éspèrer cracker ça clef.

Donc fait le calcul, si t'es cocu tu mettra peut-ètre une heure mais faudrai que ta copine soit une sacré salo…

Et si t'es pas cocu, en temps normal quoi, ben t'en aura pour au moins 2 jours à récupéré des IVS.

hs_force
a écrit le Mercredi 13 juin 2007 @21 h 12 :

Lol.. Ok mais je peux l'avoir ou cette carte spéciale?

J'ai dl winaircrackpack et déja avec airodump il me laisse pas parce que j'ai pas mis a jour les drivers de ma carte Intel pro Wireless 3945ABG j'suis sur centrino duo mais j'sais pas si y a des Wildpackets pour cette carte?

Et après jedois avoir quel programme pour sniffer les IP de mes voisins?

Merci Xorax

XoraX
a écrit le Mercredi 13 juin 2007 @22 h 07 :

Oula les cartes pour faire l'injection sous windows, je sais que ça existe mais je pourrais pas te dire… faut que t'aille voir du coté de forum.tuto-fr.com ou bien sur les forum anglais.

je sais pas pour les drivers centrino, à se qu'il parait il en ont sortit qui marche à peu près mais jamais test.

Pour sniffer tu prend ethereal ou airopeek il va bien aussi mais pour les 2 il te faut les drivers wildpacket.

Mais je compend pas pourquoi tu prend pas un live CD comme backtrack au lieu que de te prendre la tête ?

hs_force
a écrit le Jeudi 14 juin 2007 @22 h 36 :

Ok merci..

Mais j'avais lu que backtrack fonctionné que sur linux..? T'as lien pour le dl parce que sur tuto-fr.com le lien ne marche plus!

J'ai trouvé les wildpackets pour centrino sur wildpackets.com! J'vais tester.. Il faut que je fasse une copine de mes drivers original avant de modifier?

XoraX
a écrit le Vendredi 15 juin 2007 @2 h 10 :

je crois que tu n'a pas lu le tutorial. Tout y est expliqué et tu n'a rien à installer si tu tourne avec un live CD comme backtrack

Signale moi le lien mort sur tuto-fr stp je le remettrais. il y a tout sur files.tuto-fr.com

Les drivers wildpackets ne fonctionne surement pas avec le gestionnaire windows donc tu ne pourra t'en servir que pour scanner. Et donc oui, ta intéret d'avoir tes drivers original sous la main pour les remettre après

hs_force
a écrit le Dimanche 17 juin 2007 @15 h 22 :

files.tuto-fr.com quand je clike sur le lien pour Backtrack ca me dit try again et ca download pas!

Ok et j'fais comment une copie de mes drivers original? Quand j'ai acheté c'était déjà tt installé!

Merci Xorax

XoraX
a écrit le Dimanche 17 juin 2007 @22 h 51 :

Tu dois avoir un CD avec tes drivers originaux, sinon tu dois pouvoir les retrouver sur le net.

Chez moi le lien BackTrack marche nikel… éssaye dans heures où il y a moins de monde peut-être.
Je sais pas quel navigateur tu utilise mais si t'es sous IE passe à firefox, t'aura déjà plus de chance que ça marche

hs_force
a écrit le Lundi 18 juin 2007 @19 h 13 :

J'ai firefox et j'ai meme essayé avec download accelerator mais ca marche pas!

Et sur la page files.tuto-fr.com tt les soft se dl pas

Pis comment j'vais faire pour l'injection des paquets sous windows?

Merci Xorax

XoraX
a écrit le Mardi 19 juin 2007 @ 0 h 43 :

Alors là je sais pas ce que t'a… chez moi ça dl à 1Mo/s mini!!! et chez billy aussi.
sinon télécharge le ici : http://www.remote-exploit.org/backtrack_download.html

Pour l'injection sous windows j'en ai aucune idée. A se qu'il parait c'est possible mais bon je vois pas l'intéret de se prendre la tête.

fahd
a écrit le Dimanche 22 juillet 2007 @ 21 h 22 :

salut tt le monde
aircrack-ng integre dc bien l'algorythme de ptw en ajoutant la commande -z
plutot pratique:crackage de la clef wep avec 8000 Ivs seulement por ma part!!!!
Le wep,c'est FINI!

alex
a écrit le Lundi 23 juillet 2007 @ 21 h 43 :

salut

moi je veut savoir sil et possible de cracker une clé sous backtrack et aussi je suis pas très callé dans ces truc mes comment on fait pour trouver quel est notre carte :l ?

jai mon laptop et ma carte est intégré dedans

merci!

wesside-ng *contient sur le sujet* :

[…] Il s'occupe donc s'authentifier sur le réseau en regardant les clients déjà connecté. Il applique la méthode chopchop (fragmentation) et balance les paquets comme aireplay-ng. Une fois qu'il a assez de paquets ARP, il utilise l'algo de aircrack-ptw. […]

le Mercredi 12 septembre 2007 @ 22 h 42

statuquo
a écrit le Vendredi 14 septembre 2007 @ 23 h 04 :

euh … jarrive pas a compiler

je fais : bt aircrack-ptw-1.0.0 # make

mais la il affiche :

bt aircrack-ptw-1.0.0 # make

gcc -o aircrack-ptw -Wall -fomit-frame-pointer -O3 -lpcap aircrack-ptw.c aircrack-ptw-lib.c

/tmp/cconJKii.o(.text+0xaf): In function `main':

: undefined reference to `pcap_open_offline'

/tmp/cconJKii.o(.text+0xcf): In function `main':

: undefined reference to `pcap_datalink'

/tmp/cconJKii.o(.text+0×107): In function `main':

: undefined reference to `pcap_next_ex'

/tmp/cconJKii.o(.text+0x2f0): In function `main':

: undefined reference to `pcap_next_ex'

collect2: ld returned 1 exit status

make: *** [aircrack-ptw] Error 1

jai la reponse ailleur :

Troubleshooting Install:

Receiving the error on compilation:

/tmp/ccOUnQRV.o: In function 'main':

aircrack-ptw.c:(.text+0x9e): undefined reference to 'pcap_open_offline'

aircrack-ptw.c:(.text+0xb2): undefined reference to 'pcap_datalink'

aircrack-ptw.c:(.text+0xee): undefined reference to 'pcap_next_ex'

collect2: ld returned 1 exit status

make: *** [aircrack-ptw] Error 1

Fix: move -lpcap switch to the end of both gcc lines

mais comment on trouve le fichier -lpcap plz

Statuquo
a écrit le Vendredi 14 septembre 2007 @ 23 h 24 :

prob resolu

http://forums.remote-exploit.org/archive/index.php/t-6249.html

Maigret
a écrit le Mardi 23 octobre 2007 @ 11 h 21 :

Bonjour à tous, j'aimerais savoir où vous avez trouvé les drivers wildpackets pour les intel (au passage j'ai un intel centrino 3945) car sur le site officiel ils disent qu'ils sont inclus nativement dans la démo de ominpeek mais je n'ai aucun intérêt à avoir ce logiciel vu que ce sont ces drivers qui m'intéressent non?

XoraX
a écrit le Samedi 27 octobre 2007 @ 19 h 31 :

Et si, il te fodra installer le logiciel pour avoir accès à ses drivers.
une fois installé, tu devrais le désinstaller en gardant les drivers (suivant les dépendances)

Il y a des drivers expérimental qui sont sorti pour broadcom sur linux et qui permette l'injection de paquet après un patch : http://bcm43xx.berlios.de/

Mais franchement, pour le prix que ça coute une carte wifi, je te conseil plutôt d'en acheter une. tu aura des réduc avec tuto-fr.com :
http://www.tuto-fr.com/tutoriaux/carte-wifi-crack-wep-usb-pci-pcmcia.php

Zoro
a écrit le Mercredi 28 novembre 2007 @ 3 h 49 :

Salut,

Tu dis qu'on ne peut pas prendre plusieurs fichiers .cap hors chez moi ça marche… Je passe par exemple, de 22500 fichiers à 25000 après quelques secondes dans le shell aircrack. Penses-tu que cela ne change rien ?

Rikimaru
a écrit le Vendredi 11 janvier 2008 @ 23 h 38 :

Salut J'ai télécharger les pack. Ma carte reseauwifi c'est une intel wireless wifi link 4965AGN
je vouls savoirsi avec c'était possible mis ce qui me fraine c'est d'avoir lu que utiliser ce logiciel pouvais endomager mon matériel et j'ai vraiment pas envie de tuer ma carte.
Sa peut vraiment me tué mon matériel ? non parce que savoir ceasa donne pas envie lol.
Merc de ton aide.

XoraX
a écrit le Samedi 12 janvier 2008 @ 2 h 10 :

vu tout les circuits de sécurité qui existe maintenant sur les cartes mères et dans les bios, même un logiciel voulant volontairement endomager un composant serait dur à faire.
Alors un logiciel tout court… 😉

Jamais personne n'a rencontré ce genre de problème.

snake
a écrit le Samedi 12 janvier 2008 @ 20 h 00 :

salut a vous

je suis un PUR débutant et j'aimerais avoir un lien, un site ou un document m'éxpliquent tous bien se qu'il faut pour craquer un reseau wifi.

je galére surtout a trouver les bon logiciel pour manoeuvré l'opération et ou comment les installer.

merci a vous

kesy
a écrit le Dimanche 13 janvier 2008 @ 16 h 05 :

Rikimaru tu pourrais me dire quels packs as – tus download pour ta carte STP ?

Rikimaru
a écrit le Dimanche 13 janvier 2008 @ 20 h 00 :

Re Et bien 'ai télécharger le pack qui est proposé plus haut : aircrack-ptw_win32
Je ne sais pas encore si il fonctione avec ma carte reseau wifi enfaite quand j'ai voulu l'utilisé a un endroit dans l logiciel j'ai lu ce message comme quoi cela pouvais endomager e matériel car c'était a titre experimantble. Donc j'ai préférer demander avant si c'était vraiment possible. Mais vu que apparament non je vais essaer ce logiciel.
Je reviendrais vous voir car je pense pas y arriver ni qe ma care sois compatible avec le logiciel.

Rikimaru
a écrit le Mercredi 16 janvier 2008 @ 23 h 08 :

sa marche pas mes driver sont pas compatible. si vous sacer ou je peut en avoir

michmool
a écrit le Samedi 9 février 2008 @ 19 h 17 :

Franchement Backtrack ca roule… mais il faut aimer l'anglais, le comprendre et lire une cinquantaine de pages de tutos, car sans injection de paquets il faut longtemps pour les IVs
pour les apprentis linuxiens, Vous pouvez utiliser ubuntu et intaller Aircrack pack (airodump…) et l'utiliser en dual boot en virtualisation…
ce sera beaucoup plus simple que backtrack (qui est une bombe cela dit…)des explications sommaires en français (26pages qd même)
http://www.tuto-fr.com/tutoriaux/tutorial-crack-wep-aircrack.php
Pas mal, vous avez meme une liste des cartes supportées (euh certaines ne fonctionnent que sous linux)mais pour des injections de paquets plus…différentes il faut impérativement lire l'anglais.
et je remets l'adresse bt-3 beta
http://www.remote-exploit.org/backtrack_download.html

WepFarteur
a écrit le Samedi 23 février 2008 @ 21 h 37 :

Bonsoir,

Pour le problème d'utilisation sur windaub, peut-être que aircrack tournerait bien sous Cygwin (sorte d'émulateur linux)….

Obtenir la clé Wep de son voisin, c'est rigolo, mais la plupart des boxs demandent une association qui autorise la liaison d'une machine à partir de son adresse Mac. Alors à moins que vous tentez toutes les 30 secondes d'entrer sur le réseau en espérant que votre voisin appuis sur le bouton d'association, ben vous n'utiliserez jamais sa connection pour surfer….

Oui c'est vrai que la sécurité WEP n'est plus fiable puisque crackable, mais concrètement, son utilisation l'est toujours.
En pratique, si vous avez une box comme la freebox ou la livebox, vous pouvez carrément donner votre clé WEP à votre voisin et parrier l'appéro s'il réussi à utiliser votre connexion…

david
a écrit le Jeudi 3 juillet 2008 @ 10 h 29 :

salut à tous,

J'ai actuellement une carte wifi centrino 3945, mais ça ne marche pas avec airodump.
Je suis condamné à abandonner ou il suffit que j'achète une clé wifi ? Si oui laquelle est la meilleure en vue d'un crackage de clé wep ?

Merci beaucoup !

XoraX
a écrit le Vendredi 4 juillet 2008 @ 1 h 57 :

tu peux acheter une clef wifi : liste des cartes compatibles aircrack

demenvil
a écrit le Samedi 6 décembre 2008 @ 12 h 57 :

Salut moi tous c'est bien déroulé mis a part la fin…
une fois que je tape
code:

./aircrack-ptw out-0x.cap

il se note, code:

emenvil@demenvil-laptop:~/aircrack-ptw-1.0.0$ ./aircrack-ptw out-0x.cap
This is aircrack-ptw 1.0.0
For more informations see http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/

comment cela se fait-il ?

merci

barbo
a écrit le Jeudi 19 février 2009 @ 15 h 11 :

allez sur installation, c ou installation sur vista ????????? ça fait 20 ans que je bidouille, mais je m'aperçois que ça n'a pas changer, informaticien pour informaticien,vous etes dans votre partie et n'imaginer pas que d'autres ont besoin d'explications claires, en français, pas a pas, pour que n'importe qui comprenne meme le boulanger du coin, tiens donner moi la recette de la pate a pain dans les bonnes proportions puisque vous pensez que lorsqu'on ne comprend pas on est tous des cons, vous savez réparer votre bagnole vous ??? si c pas votre philisophie
d'aider des ignares qui ne demande qu'a apprendre, pourquoi faites vous des blogs ???????

WEPBuster : crack WEP automatique *contient sur le sujet* :

[...] deauth, changement d'adresse MAC, récupération de IVs, crackage de la clef WEP avec aircrack-ptw. Une commande à lancer et vous avez plus qu'à vous tourner les pouces. Aircrack pour les [...]

le Mardi 9 juin 2009 @ 5 h 25

boboss
a écrit le Lundi 3 août 2009 @ 22 h 45 :

ben j ai une question, je m demande si c possible de crack une clé wep avc son telephone portable, je sais pas si c fesable ou pas si c fesable comment et kel sont les logiciel adequat et o fait j ai nokia N78 on c jamais si ca peut aide merci d avance

vantura
a écrit le Samedi 12 décembre 2009 @ 12 h 29 :

je voudrais aussi de l'aide pour l'installation de aircrack-ng sous windows

z-la
a écrit le Samedi 12 juin 2010 @ 12 h 58 :

bonjour,
moi aussi jai un probleme je narive pas a le télécharger
et j'ai un ordinateur acer

avec le Netgear n-300

comment je peux faire merciii

HACK
a écrit le Vendredi 3 septembre 2010 @ 9 h 20 :

HEY GANG DE CAVE!!!!!! HELLO BOOT CD BACK|TRACK 4R1 EN 2 MIN TOUT LES CLÉ DÉ RÉSSAUX CAPTÉ \!@#$&?

kenza
a écrit le Mercredi 31 août 2011 @ 17 h 18 :

Wach Fiiih 3 ans DIyal Lhebss Li telechargah????

kenza
a écrit le Mercredi 31 août 2011 @ 17 h 21 :

La personne Ki telecharge ce logiciel doit se prisonier 3 ans????? c est vraiiiiiiiiix??

kenza
a écrit le Mercredi 31 août 2011 @ 17 h 24 :

attenntionnnnnnnnnnnnnnnnn 3 ans de prison a ceux ki telechrge ce logoiceil moi je l ai telecharger puis je l ai suprimer

Laissez un commentaire :

Nom (requis)

Mail (ne sera pa publié) (requis)

Site Web

Recevoir les nouveaux commentaires par email.

Envoyer le commentaire

Syndicate this site using RSS
Articles, Commentaires.

CERTAINS DROITS RESERVES

Powered by WordPress